Dec 06 2023

NETMANAGEIT

Intelligence Report

DanaBot Triage

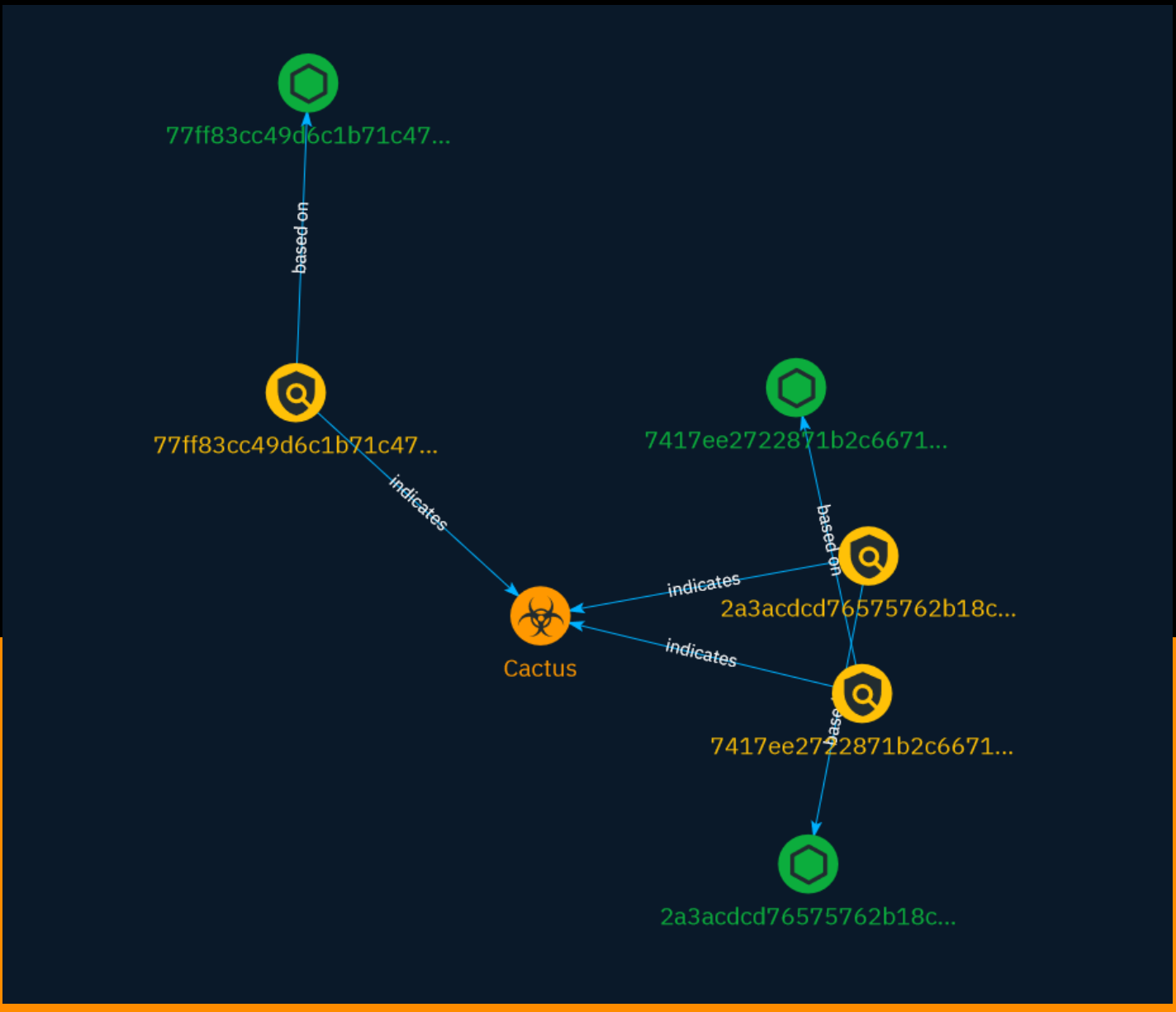

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A look at a sample of the Danabot malware loader and its core component, following a report from Microsoft's Esentire report on the threat posed by the Storm-0216 ransomware.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Indicator

Name

7417ee2722871b2c667174acc43dd3e79fcdd41bef9a48209eeae0ed43179e1f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7417ee2722871b2c667174acc43dd3e79fcdd41bef9a48209eeae0ed43179e1f']

Name

77ff83cc49d6c1b71c474a17eeaefad0f0a71df0a938190bf9a9a7e22531c292

Description

Trojan:Win64/UACBypassExp.A!MTB

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '77ff83cc49d6c1b71c474a17eeaefad0f0a71df0a938190bf9a9a7e22531c292']

Name

2a3acdcd76575762b18c18c644a745125f55ce121f742d2aad962521bc7f25fd

Description

sdd.dll

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2a3acdcd76575762b18c18c644a745125f55ce121f742d2aad962521bc7f25fd']

Malware

Name
Cactus

StixFile

Value
2a3acdcd76575762b18c18c644a745125f55ce121f742d2aad962521bc7f25fd
7417ee2722871b2c667174acc43dd3e79fcdd41bef9a48209eeae0ed43179e1f
77ff83cc49d6c1b71c474a17eeaefad0f0a71df0a938190bf9a9a7e22531c292

External References

- https://otx.alienvault.com/pulse/657084bd049779d60bad9a49
- https://research.openanalysis.net/danabot/loader/delphi/2023/12/04/danabot.html